Listing of Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application.

1. - 183. (Canceled).

184. (Previously presented) The method as recited in claim 258 wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the inputted recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the inputted recipient data included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

185. (Previously presented) The method as in claim 236, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

186. (Previously presented) The method as in claim 236, wherein said access event comprises access of an e-mail account associated with said recipient e-mail address.

187. (Previously presented) The method as in claim 236, wherein said access event comprises activation of an e-mail processing software associated with said recipient e-mail address.

188. (Previously presented) The method as in claim 236, wherein the step of transmitting an e-mail from a sender computer includes attaching an executable attachment file in conjunction with

the e-mail, the executable attachment file having a first module for prompting the party who requested said access event to enter recipient data; and

and wherein the step of detecting an access event includes the step of executing the first module of the executable attachment file.

189. (Previously presented) The method as in claim 188, wherein the executable attachment file has a second module transmitted and delivered therewith, the second module for detecting the access event, and further comprising the step of automatically executing the second module upon delivery of the attachment file to the recipient e-mail address.

190. (Canceled).

191. (Previously presented) The method as in claim 236, wherein said recipient e-mail address is associated with a recipient computer.

192. (Previously presented) The method as in claim 191, wherein said recipient computer is a server of a service provider.

193. (Previously presented) The method as in claim 191, wherein said recipient computer is a user system that is directly accessible by a recipient, said user system including electronic mail processing software.

194. (Previously presented) The method as in claim 236 , wherein said inputted recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

195. (Previously presented) The method as in claim 236, wherein said inputted recipient data comprises identity information that identifies an individual.

196. (Previously presented) The method as in claim 195, wherein said identity information pertains to biometric identification.

197. (Previously presented) The method as in claim 196 further comprising the step of recognizing biometric attributes of an individual.

198. (Previously presented) The method as in claim 195, wherein said identity information includes alphanumeric text identification information.

199. (Previously presented) The method as in claim 236 , wherein said inputted recipient data comprises information that identifies a business.

200. (Previously presented) The method as in claim 236, wherein said inputted recipient data comprises information that identifies an organization.

201. (Previously presented) The method as in claim 236 , wherein said inputted recipient data comprises a computer generated user code.

202. (Previously presented) The method as in claim 236 further including the step of sending access event data of attendant conditions of said access event.

203. (Previously presented) The method as in claim 236 , wherein said recipient is an individual.

204. (Previously presented) The method as in claim 236, wherein said recipient is a business.

205. (Previously presented) The method as in claim 236, wherein said recipient is an organization.

206. (Previously presented) The method as in claim 236, wherein said inputted recipient data is used to verify proper delivery of legal documents.

207. (Previously presented) The method as in claim 236, wherein said inputted recipient data is used to verify proper delivery of confidential documents.

208. (Previously presented) The method recited by claim 260 wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the acquired recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the acquired recipient data contained with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

209. (Previously presented) The method as in claim 260, wherein said access event comprises access of said e-mail that was delivered to said recipient e-mail address.

210. (Previously presented) The method as in claim 260, wherein said access event comprises access of an e-mail account associated with said recipient e-mail address.

211. (Previously presented) The method as in claim 260, wherein said access event comprises activation of e-mail processing software associated with said recipient e-mail address.

212. (Previously presented) The method as in claim 260, wherein the step of transmitting an e-mail from a sender computer includes attaching an executable attachment file in conjunction with the e-mail, the executable attachment file having a first module for acquiring recipient data that is related to biometric identification of the recipient, and

wherein the step of detecting an access event includes the step of executing the first module of the executable attachment file.

213. (Previously presented) The method as in claim 212, wherein the executable attachment file has a second module transmitted and delivered therewith, the second module for detecting the access event, and further comprising the step of:

automatically executing the second module upon delivery of the attachment file to the recipient e-mail address.

214. Canceled.

215. (Previously presented) The method as in claim 260 , wherein said recipient e-mail address is associated with a recipient computer.

216. (Previously presented) The method as in claim 215, wherein said recipient computer is a server of a service provider that is capable of receiving e-mail.

217. (Previously presented) The method as in claim 215, wherein said recipient computer is a user system that is directly accessible by the recipient, said user system including electronic mail processing software and being capable of receiving e-mail.

218. (Previously presented) The method as in claim 260, wherein said acquired recipient data is related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

219. (Previously presented) The method as in claim 260, wherein said acquired recipient data comprises identity information that identifies an individual.

220. (Previously presented) The method as in claim 260 further comprising means for recognizing biometric attributes of an individual.

221. (Previously presented) The method as in claim 260, wherein said acquired recipient data comprises information that identifies a business.

222. (Previously presented) The method as in claim 260, wherein said acquired recipient data comprises information that identifies an organization.

223. (Previously presented) The method as in claim 260, wherein said acquired recipient data comprises a computer generated user code.

224. (Previously presented) The method as in claim 260 further including the step of sending access event data of conditions attendant said access event.

225. (Previously presented) The method as in claim 260, wherein said recipient is an individual.

226. (Previously presented) The method as in claim 260, wherein said recipient is a business.

227. (Previously presented) The method as in claim 260, wherein said recipient is an organization.

228. (Previously presented) The method as in claim 260, wherein said sent recipient data is used to verify proper delivery of legal documents.

229. (Previously presented) The method as in claim 260, wherein said sent recipient data is used to verify proper delivery of confidential documents.

230. (Canceled).

231. (Previously presented) The method as in claim 260, wherein said recipient data is acquired as a requisite condition for permitting access to said delivered e-mail.

232. (Previously presented) The method as in claim 260, wherein said recipient data is acquired as a requisite condition for permitting access to said recipient e-mail address.

233. (Previously presented) The method as in claim 260, wherein said recipient data is acquired as a requisite condition for operating a remote user computer, said remote user computer being operable to gain access to said recipient e-mail address.

234. (Previously presented) The method as in claim 260, wherein said recipient data is comprised of alphanumeric text, said alphanumeric text being associated with the at least one biometric attribute of said recipient.

235. (Canceled).

236. (Currently amended) A method for verifying whether an e-mail received by a recipient was accessed by an intended recipient, said method comprising:

a) receiving an e-mail ~~into~~ at a recipient e-mail address;

b) detecting an access event, and prompting the party associated with said access event to input recipient data prior to allowing the requested access, said recipient data including identifying data related to the party associated with said requested access;

c) permitting said e-mail to be accessed after the party associated with said access event inputs said recipient data; and

d) sending identifying data relating to the party associated with said access event for reference by a sending party to identify the party who accessed said e-mail.

237. (Previously presented) The method recited by claim 264 wherein the step of sending data that identifies said recipient for confirming proper delivery of said e-mail includes the steps of :

a) generating a confirmation of receipt notice wherein the data that identifies the recipient is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the data that identifies the recipient that is included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the email was accessed by the intended recipient.

238. (Previously presented) The method as in claim 264, wherein said data that identifies said recipient is related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

239. (Previously presented) The method as in claim 264, wherein the data that identifies said recipient is comprised of alphanumeric text, said alphanumeric text being associated with ~~the~~ at least one biometric attribute of said recipient.

240. (Previously presented) The method as in claim 264 further including the step of recognizing biometric attributes of an individual.

241. (Previously presented) The method as in claim 264, wherein said data that identifies said recipient comprises identity information that identifies an individual.

242. (Previously presented) The method as in claim 264, wherein said data that identifies said recipient comprises information that identifies a business.

243. (Previously presented) The method as in claim 264, wherein said data that identifies said recipient comprises information that identifies an organization.

244. - 247. (Canceled).

248. (Currently amended) A system for verifying whether e-mail received by a recipient was accessed by an intended recipient, said system comprising:

a) a recipient computer connected to a communications network, said recipient computer capable of receiving an e-mail and further having data storage for storing said received e-mail;

b) software on a computer storage medium capable of detecting an access event, wherein, upon detecting said access event, said software prompts the party associated with said access event to input recipient data prior to allowing the requested access and wherein said software further permits said e-mail to be accessed after the party associated with said access event inputs said recipient data, said recipient data comprising identifying data related to the party associated with said requested access; and

c) means for sending identifying data relating to the party associated with said access event to identify the party who accessed said e-mail.

249. (Previously presented) The system as in claim 248, wherein said access event comprises access of a delivered e-mail.

250. (Previously presented) The system as in claim 248, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

251. (Previously presented) The system as in claim 248, wherein said access event comprises activation of e-mail processing software associated with the e-mail address to which said e-mail was delivered.

252. (Currently amended) A system for verifying whether e-mail received by a recipient was accessed by an intended recipient, said system comprising:

a) a recipient computer connected to a communications network, said recipient computer being capable of receiving an e-mail and further having data storage for storing said received e-mail;

b) biometric identification means for recognizing biometric attributes of an individual;

c) software on a computer storage medium capable of detecting an access event and identifying an individual associated with said access event through utilization of inputted biometric attributes of said individual, said software permitting said e-mail to be accessed after input of said biometric attributes of the individual associated with said access event; and

d) means for sending data that identifies said individual for identifying the party who accessed said e-mail.

253. (Previously presented) The system as in claim 252, wherein said access event comprises access of a delivered e-mail.

254. (Previously presented) The system as in claim 252, wherein said access event comprises access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

255. (Previously presented) The system as in claim 252, wherein said access event comprises activation of ~~the~~ e-mail processing software associated with the e-mail address to which said e-mail was delivered.

256. - 257. (Canceled).

258. (Previously presented) A method for verifying whether an e-mail received by a recipient was accessed by an intended recipient, said method comprising:

a) receiving an e-mail into a recipient e-mail address;

b) detecting an access event, and prompting the party that requested said access to input recipient data prior to allowing the requested access, said recipient data including identifying data that is associated with the party that requested said access;

c) permitting said e-mail to be accessed after the party that requested said access inputs said recipient data; and

d) sending identifying data relating to the party that requested said access event to identify the party who accessed said e-mail.

259. (Previously presented) The method recited by claim 236 wherein said step of sending recipient data for confirming proper delivery of said e-mail includes the steps of:

a) generating a confirmation of receipt notice wherein the inputted recipient data is included with said confirmation of receipt notice; and

b) sending said confirmation of receipt notice, wherein the inputted recipient data included with said confirmation of receipt notice can be compared to information associated with said intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

260. (Previously presented) A method for verifying whether e-mail received by a recipient was accessed by an intended recipient, said method comprising:

a) receiving an e-mail into a recipient e-mail address;

b) detecting an access event;

c) acquiring recipient data that is related to biometric identification of the recipient;

d) permitting said e-mail to be accessed after acquiring said recipient data; and

e) sending identifying data related to biometric identification of said recipient for identifying the recipient of of said e-mail.

261. (Previously presented) The method as recited in claim 260 wherein said recipient data is acquired prior to said access event.

262. (Previously presented) The method as recited in claim 260 wherein said recipient data is acquired after said access event.

263. (Previously presented) The method as recited in claim 260 wherein said recipient data is sent to an e-mail address.

264. (Previously presented) A method for verifying whether e-mail received by a recipient was accessed by an intended recipient, said method comprising:

a) receiving an e-mail into a recipient e-mail address;

b) identifying a recipient utilizing biometric identification;

c) detecting an access event;

d) permitting said e-mail to be accessed after acquiring said biometric identification; and

e) sending data related to said biometric identification of said recipient for confirming proper delivery of said e-mail.

265. (Previously presented) The method as recited in claim 264 wherein said recipient is identified prior to said access event.

266. (Previously presented) The method as recited in claim 264 wherein said recipient is identified after said access event.

267. (Previously presented) The method as recited in claim 264 wherein said data that identifies said recipient is sent to an e-mail address.

268. (Previously presented) A method for verifying whether e-mail received by a recipient was accessed by an intended recipient, said method comprising:

a) receiving an e-mail into a recipient e-mail address;

b) identifying a recipient in association with biometric identification;

c) detecting an access event;

d) permitting said e-mail to be accessed after acquiring said biometric identification; and

e) sending data related to said biometric identification of said recipient for confirming proper delivery of said e-mail.

269. (Previously presented) The method as in claim 268 wherein said recipient is identified prior to said access event.

270. (Previously presented) The method as in claim 268 wherein said recipient is identified after said access event.

271. (Previously presented) The method as in claim 268 wherein said data that identifies said recipient is sent to an e-mail address.

272. - 278. (Canceled).

279. (Previously presented) The system as in claim 252, wherein said data that identifies said individual for confirming proper delivery of said e-mail is sent to an e-mail address.

280. - 326. (Canceled).

327. (Previously presented) The method as in claim 236, wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

328. (Previously presented) The method as in claim 236, wherein a remote user computer may be used to gain remote access to said recipient e-mail address.

329. (Previously presented) The method as in claim 236 wherein the party that is associated with said access event is an individual.

330. (Previously presented) The method as in claim 236 wherein the party that is associated with said access event is a business.

331. (Previously presented) The method as in claim 236 wherein the party that is associated with said access event is an organization.

332. (Previously presented) The method as in claim 258 wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

333. (Previously presented) The method as in claim 184, wherein said confirmation of receipt notice is sent to an e-mail address.

334. (Previously presented) The method as in claim 258, wherein said inputted recipient data pertains to alphanumeric text identification, biometric identification, password identification, a computer generated user code, or a combination thereof.

335. (Previously presented) The method as in claim 208, wherein said confirmation of receipt notice is sent to an e-mail address.

336. (Previously presented) The method as in claim 260, wherein a remote user computer may be used to gain remote access to said recipient e-mail address.

337. (Previously presented) The method as in claim 219, wherein said identity information includes alphanumeric text identification.

338. (Previously presented) The method as in claim 237, wherein said confirmation of receipt notice is sent to an e-mail address.

339. (Previously presented) The method as in claim 268 , wherein said data that identifies said recipient is related to a biometric imprint, alphanumeric text identification, password identification, a computer generated user code, or a combination thereof.

340. (Previously presented) The method as in claim 268 further comprising the step of recognizing biometric attributes of an individual.

341. - 345. (Canceled).

346. (Previously presented) The system as in claim 248, wherein said recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

347. (Previously presented) The system as in claim 252, wherein said individual is identified prior to said access event.

348. (Previously presented) The system as in claim 252, wherein said individual is identified after said access event.